

DETAILED ACTION

This Examiner's Amendment and Examiner's Reasons for Allowance action is in response to the filing of 10/26/2009.

Examiner Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Thomas Lane on 01/18/2010.

- The application has been amended as follows:
Claims 15-19 (Cancelled).

Allowance

2. Claims 1-7, 9-19, & 21-41 have been cancelled.

3. Claims 8 & 20 have been amended with written arguments which overcome the examiner's prior rejections and objections, see paper of 07/24/2009. Examiner withdraws all outstanding rejections and objections to claims 8 & 20.
4. Claims 8 & 20 are allowed.

Examiner's Statement of Reasons for Allowance

5. Prior art was found which disclosed high speed encryption system and method [e.g. Bianco et al. (US-5365588-A)] and authentication engine architecture and method [e.g. Buer et al. (US-20020001384-A1)] and [e.g. M.J.B. Robshaw ("On Recent Results for MD2, MD4, and MD5")].
6. The following is an examiner's statement of reasons for allowance:
 - The prior art of record does not teach or render obvious the limitations as recited in independent Claims 8 & 20, specific to "a plurality of pipeline stages to perform an inner loop of a hash algorithm" and "the plurality of pipeline stages comprising at least as many pipeline stages as there are iterations of the inner loop to be performed and as many pipeline stages as there are chaining variable to be used in the inner loop" and "control logic to schedule operations to be executed within the plurality of pipeline stages" and "operations are to be scheduled by the control logic and executed by the plurality of pipeline stages so as to minimize data dependencies between iterations of the inner loop

to be performed” and “...and is to be performed at an operating frequency equal to that of the adder”.

- Therefore, the Examiner considers both the above limitations in combination with the remaining limitations of each respective independent claim, as applied to implementing a security algorithm, as the non-obvious novelties of the invention.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance”.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private

Art Unit: 2436

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OSCAR A LOUIE/
01/19/2010

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436